

|  |
| --- |
| X-ROAD 6.0  Configuration Proxy Manual  2.0 |
|  |

Version History

|  |  |  |
| --- | --- | --- |
| Date | Version | Description |
| 26.11.2014 | 1.0 | Initial version |
| 19.01.2015 | 1.1 | License information added |
| 07.05.2015 | 1.2 | Configuration properties table added |
| 26.05.2015 | 1.3 | Token initialization description added |
| 30.06.2015 | 1.4 | Minor corrections done |
| 09.07.2015 | 1.5 | Repository address updated |
| 20.09.2015 | 2.0 | Editorial changes made |

Table of Contents

[1 Introduction 4](#_Toc430620737)

[1.1 Target Audience 4](#_Toc430620738)

[1.2 X-Road Configuration Proxy 4](#_Toc430620739)

[2 Installation 5](#_Toc430620740)

[2.1 Supported Platforms 5](#_Toc430620741)

[*2.2* Reference Data 5](#_Toc430620742)

[2.3 Requirements for the Configuration Proxy 5](#_Toc430620743)

[2.4 Preparing OS 6](#_Toc430620744)

[2.5 Installation 6](#_Toc430620745)

[2.6 Post-Installation Checks 6](#_Toc430620746)

[2.7 Installing the Support for Hardware Tokens 7](#_Toc430620747)

[3 Configuration 8](#_Toc430620748)

[3.1 Prerequisites 8](#_Toc430620749)

[3.1.1 Security Token Activation 8](#_Toc430620750)

[3.1.2 User Access Privileges 8](#_Toc430620751)

[3.2 General Configuration 8](#_Toc430620752)

[3.2.1 Configuration Structure of the Instances 9](#_Toc430620753)

[3.3 Proxy Instance Reference Data 10](#_Toc430620754)

[3.4 Proxy Instance Configuration 10](#_Toc430620755)

[3.5 Additional Configuration 12](#_Toc430620756)

[3.5.1 Changing the Validity Interval 12](#_Toc430620757)

[3.5.2 Deleting the Signing Keys 12](#_Toc430620758)

[3.5.3 Changing the Active Signing Key 12](#_Toc430620759)

# Introduction

## Target Audience

The intended audience of this Manual are X-Road system administrators responsible for installing and using X-Road configuration proxy software.

The document is intended for readers with a moderate knowledge of Linux server management, computer networks, and the X-Road working principles.

## X-Road Configuration Proxy

The configuration proxy acts as an intermediary between X-Road servers in the matters of global configuration exchange.

The goal of the configuration proxy is to download an X-Road global configuration from a provided configuration source and further distribute it in a secure way. Optionally, the downloaded global configuration may be modified to suit the requirements of the configuration proxy owner.

The configuration proxy can be configured to mediate several global configurations (from multiple configuration sources).

# Installation

## Supported Platforms

The configuration proxy runs on the *Ubuntu Server 14.04 Long-Term Support (LTS)* operating system on a 64-bit platform. The configuration proxy's software is distributed as .deb packages through the official X-Road repository at [http://x-road.eu](http://x-road.eu/)

The software can be installed both on physical and virtualized hardware (of the latter, Xen and Oracle VirtualBox have been tested).

## Reference Data

*Note*: The information in empty cells has to be determined before the server’s installation, by the person performing the installation.

Caution: Data necessary for the functioning of the operating system is not included.

|  |  |  |  |
| --- | --- | --- | --- |
| Ref |  | | Explanation |
| 1.0 | Ubuntu 14.04, 64bit  2GB RAM, 3GB free disk space | | Minimum requirements |
| 1.1 | http://x-road.eu/packages | | X-Road package repository |
| 1.2 | http://x-road.eu/packages/xroad\_repo.gpg | | The repository’s key |
| 1.3 | TCP 80 | global configuration distribution | Ports for inbound connections (from the external network to the configuration proxy) |
| 1.4 | TCP 80 | global configuration download | Ports for outbound connections (from the configuration proxy to the external network) |
| 1.5 |  | | Configuration proxy’s public IP address, NAT address |

## Requirements for the Configuration Proxy

Minimum recommended hardware parameters:

* the server’s hardware (motherboard, CPU, network interface cards, storage system) must be supported by Ubuntu 14.04 in general;
* a 64-bit dual-core Intel, AMD or compatible CPU; AES instruction set support is highly recommended;
* 2 GB RAM;
* a 100 Mbps network interface card;
* if necessary, interfaces for the use of hardware tokens.

Requirements to software and settings:

* an installed and configured Ubuntu 14.04 LTS x86-64 operating system;
* if the configuration proxy is separated from other networks by a firewall and/or NAT, the necessary connections to and from the security server must be allowed (reference data: 1.3; 1.4). The enabling of auxiliary services which are necessary for the functioning and management of the operating system (such as DNS, NTP, and SSH) is outside the scope of this guide;
* if the configuration proxy has a private IP address, a corresponding NAT record must be created in the firewall (reference data: 1.5).

## Preparing OS

Set operating system locale. Add following line to /etc/environment file:  
LC\_ALL=en\_US.UTF-8

## Installation

To install the X-Road configuration proxy software, follow these steps.

1. Add to /etc/apt/sources.list the address of X-Road package repository (reference data: 1.1) and the nginx repository:  
     
   deb http://x-road.eu/packages trusty main  
   deb http://ppa.launchpad.net/nginx/stable/ubuntu trusty main  
   deb http://ppa.launchpad.net/openjdk-r/ppa/ubuntu trusty main
2. Add the X-Road repository’s signing key to the list of trusted keys (reference data: 1.2):

curl http://x-road.eu/packages/xroad\_repo.gpg | sudo apt-key add –  
sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 00A6F0A3C300EE8C  
sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys EB9B1D8886F44E2A

1. Issue the following commands to install the configuration proxy packages:  
     
   sudo apt-get update  
   sudo apt-get install xroad-confproxy

## Post-Installation Checks

The installation is successful if the 'xroad-signer' service is started, the 'xroad-confproxy' cron job is added, and the configuration proxy management utilities are available from the command line.

* Check from the command line that the 'xroad-signer' service is in the start/running state (example output follows):  
    
  sudo initctl list | grep "^xroad-"  
    
  xroad-signer start/running, process 19393
* Check from the command line that the 'xroad-confproxy' cron job is present (example output follows):  
    
  sudo ls /etc/cron.d/ | grep "^xroad-"  
    
  xroad-confproxy
* Make sure that the following commands are available from the command line:  
    
  signer-console  
  confproxy-view-conf  
  confproxy-create-instance  
  confproxy-add-signing-key  
  confproxy-del-signing-key  
  confproxy-generate-anchor

## Installing the Support for Hardware Tokens

Installation of hardware token vendorspecific library and configuration of tokens is not in scope of this documentation. Vendorspecific support for PKCS#11API must be present before proceeding.

If you intend to use hardware tokens with the system (smartcard, USB token, Hardware Security Module), the hardware token support module must be installed. Use the following command:

sudo apt-get install xroad-addon-hwtokens

Vendorspecific library name is configured in /etc/xroad/devices.ini file.

After installation and configuring library, the xroad-signer service must be restarted:

sudo service xroad-signer restart

# Configuration

To start using the configuration proxy, a proxy instance configuration needs to be created. Several proxy instances can be configured to mediate multiple global configurations.

## Prerequisites

### Security Token Activation

The configuration proxy uses a security token for storing the key that is used for signing the distributed configuration. The token can be stored either on hard disk (software token) or in hardware. Before the configuration proxy can be used, the security token must be initialized and activated.

Initialization of a software token can be done as follows:

signer-console init-software-token signer-console list-tokens

A PIN is prompted, which will be used to log in to the software token afterwards. Initialization of hardware tokens is vendorspecific and is not in scope of this documentation.

Activation of the security token is done by logging in to the token, using the following command:

signer-console login-token <TOKEN\_ID>

where <TOKEN\_ID> is the identifier of the security token, which can be found with:

signer-console list-tokens

Note, that the identifier of a software token is always „0”.

### User Access Privileges

The administrator must execute configuration scripts as the 'xroad' user.

## General Configuration

Modify '/etc/xroad/conf.d/local.ini' to contain the following:

[configuration-proxy]

; Address of the webserver serving the distributed configuration   
address=<public or NAT address>

The configuration of this parameter is necessary for generating a correctly formatted configuration anchor file that will need to be uploaded to central servers that should receive configurations mediated by this proxy, this process is described in detail in 3.4 . There are several more system parameters that can be configured in '/etc/xroad/conf.d/local.ini' under the 'configuration-proxy' section, their descriptions and default values can be seen from the following table:

|  |  |  |
| --- | --- | --- |
| Parameter | Default value | Explanation |
| address | 0.0.0.0 | The public IP or NAT address (reference data: 1.5) which can be accessed for downloading the distributed global configurations. |
| configuration-path | /etc/xroad/confproxy/ | Absolute path to the directory containing the configuration files of the proxy instance. The format of the configuration directory is described in 3.2.1 . |
| generated-conf-path | /var/lib/xroad/public | Absolute path to the public web server directory where the global configuration files generated by this configuration proxy, should be placed for distribution. |
| signature-algorithm-id | SHA512withRSA | ID of the algorithm the configuration proxy should use when computing global configuration signatures. The possible values are: SHA256withRSA, SHA384withRSA, SHA512withRSA |
| hash-algorithm-uri | http://www.w3.org/2001/04/xmlenc#sha512 | URI identifying the algorithm the configuration proxy should use to calculate hash values for the global configuration file. The possible values are: http://www.w3.org/2001/04/xmlenc#sha256, http://www.w3.org/2001/04/xmlenc#sha512 |
| download-script | /usr/share/xroad/scripts/download\_instance\_configuration.sh | Absolute path to the location of the script that initializes the global configuration download procedure. |

The configuration proxy is periodically started by a cron job. It reads the properties described above, from the configuration file before executing each proxy instance configured in 'configuration-path', generating new global configuration directories using algorithms as defined by 'signature-algorithm-id' and 'hash-algorithm-uri'. The generated directories are subsequently placed in 'generated-conf-path' for distribution.

### Configuration Structure of the Instances

Each global configuration that is to be mediated by the configuration proxy requires a proxy instance to be configured. The configuration of a proxy instance consists of a set of configuration files, including

* a trusted anchor .xml of the configuration being mediated;
* a configuration .ini file;
* verification certificates for the configured signing keys.

The following example file tree shows configured proxy instances named PROXY1 and PROXY2:

<configuration-path>/

|-PROXY1/

| |-cert\_QWERTY123.pem

| |-cert\_321YTREWQ.pem

| |-conf.ini

| `-anchor.xml

|-PROXY2/

| |-cert\_1234567890.pem

| |-conf.ini

| `-anchor.xml

`-...

The configuration of proxy instances is described in 3.4 .

## Proxy Instance Reference Data

ATTENTION: The names in the angle brackets<> are chosen by the X-Road configuration proxy administrator.

|  |  |  |
| --- | --- | --- |
| Ref |  | Explanation |
| 2.1 | <PROXY\_NAME> | Name of the proxy instance being configured |
| 2.2 | <SECURITY\_TOKEN\_ID> | ID of a security token (as defined by prerequisites 3.1 ) |
| 2.3 | <ANCHOR\_FILENAME> | Filename of the generated anchor .xml file that the configuration proxy clients will need to use for downloading the global configuration |

## Proxy Instance Configuration

1. Create configuration files for the new proxy instance by invoking the 'confproxy-create-instance -p <PROXY\_NAME>' command. Afterwards, use the 'confproxy-view-conf -p <PROXY\_NAME>' command to verify that the operation has been successfully completed (example output follows):

confproxy-create-instance -p PROXY

Populating 'conf.ini' with default values.

Done.

confproxy-view-conf -p PROXY

Configuration for proxy 'PROXY'

Validity interval: 600 s.

anchor.xml

================================================

'anchor.xml' could not be loaded: IOError: /etc/xroad/confproxy/PROXY/anchor.xml (No such file or directory)

Configuration URL

================================================

http://1.2.3.4/PROXY/conf

Signing keys and certificates

================================================

active-signing-key-id:

NOT CONFIGURED (add 'active-signing-key-id' to 'conf.ini')

1. Generate a signing key and a self signed certificate for the newly created proxy instance using the following command:

confproxy-add-signing-key -p <PROXY\_NAME> -t <SECURITY\_TOKEN\_ID>

If no active signing key is configured for the proxy instance, then the new key should be set as the currently active key (example output follows):

confproxy-add-signing-key -p PROXY -t 0

Generated key with ID QWERTY123

No active key configured, setting new key as active in conf.ini

Saved self-signed certificate to cert\_QWERTY123.pem

confproxy-view-conf -p PROXY  
...

Signing keys and certificates

================================================

active-signing-key-id:

QWERTY123 (Certificate: /etc/xroad/confproxy/PROXY/cert\_QWERTY123.pem)

Alternatively, one may add an existing key using the '–k <KEY\_ID>' argument:

confproxy-add-signing-key -p PROXY -k QWERTY123

No active key configured, setting new key as active in conf.ini

Saved self-signed certificate to cert\_QWERTY123.pem

1. To define which global configuration this proxy instance should distribute, download the source anchor from a X-Road central server and save it as '/etc/xroad/confproxy/<PROXY\_NAME>/anchor.xml'.
2. The configuration proxy should be operational at this point. The periodic cron job (once a minute) should download the global configuration defined in '/etc/xroad/confproxy/<PROXY\_NAME>/anchor.xml' and generate a directory for distribution. The output of 'confproxy-view-conf -p <PROXY\_NAME>' should be similar to the following:

confproxy-view-conf -p PROXY  
  
Configuration for proxy 'PROXY'

Validity interval: 600 s.

anchor.xml

================================================

Instance identifier: AA

Generated at: UTC 2014-11-17 09:28:56

Hash: 3A:3D:B2:A4:D3:FC:E8:08:7E:EA:8A:92:5C:6E:92:0C:70:C8

Configuration URL

================================================

http://1.2.3.4/PROXY/conf

Signing keys and certificates

================================================

active-signing-key-id:

QWERTY123 (Certificate: /etc/xroad/confproxy/PROXY/cert\_QWERTY123.pem)

1. To let clients download the generated global configuration an anchor file needs to be generated using the following command:

confproxy-generate-anchor -p <PROXY\_NAME> -f <ANCHOR\_FILENAME>

If generation was successful the output should be simply:

confproxy-generate-anchor -p PROXY -f anchor.xml

Generated anchor xml to 'anchor.xml'

1. To make sure that the global configuration is being distributed correctly use the '/usr/share/xroad/scripts/download\_instance\_configuration.sh' script, giving it <ANCHOR\_FILENAME> and the path, which should hold the downloaded files, as arguments (example output follows):

mkdir test\_download

/usr/share/xroad/scripts/download\_instance\_configuration.sh anchor.xml test\_download/  
  
... - Downloading configuration from http://1.2.3.4/PROXY/conf

... - Downloading content from http://1.2.3.4/PROXY/123/AA/shared-params.xml

... - Saving SHARED-PARAMETERS to test\_download/AA/shared-params.xml

... - Saving content to file test\_download/AA/shared-params.xml

... - Downloading content from http://1.2.3.4/PROXY/123/AA/private-params.xml

... - Saving PRIVATE-PARAMETERS to test\_download/AA/private-params.xml

... - Saving content to file test\_download/AA/private-params.xml

If the proxy instance has been configured correctly, the 'test\_download' directory should contain the downloaded global configuration files.

## Additional Configuration

### Changing the Validity Interval

There is an additional property in the configuration file of the proxy instance (/etc/xroad/confproxy/<PROXY\_NAME>/conf.ini) that determines the validity interval of the generated global configuration for a given instance.

The default value is 10 minutes (600 seconds). The property is set by modifying the following field in the configuration file:

[configuration-proxy]

...

validity-interval-seconds=600

Notice that when the configuration proxy instance is started, it deletes all the previously generated global configuration directories that are older than the currently configured validity interval for that instance.

### Deleting the Signing Keys

Should a signing key need to be deleted, the following command can be used:

configuration-del-signing-key -p <PROXY\_NAME> -k <SIGNING\_KEY\_ID>

where <SIGNING\_KEY\_ID> can be found in the output of 'confproxy-view-conf' (example output follows):

confproxy-del-signing-key -p PROXY -k QWERTY123  
  
Deleted key from signer

Deleted key from conf.ini

Deleted self-signed certificate 'cert\_QWERTY123.pem'

Attempts to delete the active signing key will be unsuccessful.

### Changing the Active Signing Key

Additional signing keys can be added with the following command:

confproxy-add-signing-key -p <PROXY\_NAME> -t <SECURITY\_TOKEN\_ID>

Keys added in this manner will be marked as inactive keys ('signing-key-id-\*=<KEY\_ID>') in the proxy instance configuration file (/etc/xroad/confproxy/<PROXY\_NAME>/conf.ini). In case the current active signing key has to be replaced by one of the additional keys, the configuration file of the proxy instance will need to be modified, changing the following lines:

[configuration-proxy]

...

active-signing-key-id=QWERTY123

signing-key-id-1=QWERTY123

signing-key-id-2=321YTREWQ

to the following ones:

[configuration-proxy]

...

active-signing-key-id=321YTREWQ

signing-key-id-1=QWERTY123

signing-key-id-2=321YTREWQ

After the change the key 'QWERTY123' may be deleted if necessary.